Applicant : Marinus Frans Kaashoek et al.   Attorney's Docket No.: 12221-005001
Serial No. : 09/931,291
Filed   : August 16, 2001
Page   : 6 of 8

REMARKS

Claims 1, 9 and 18 have been amended to clarify language in the claims and more distinctly claim the invention. For instance, claim 1 now recites "control center" rather than central controller system.

The Examiner rejected claims 1-6, 9-13, and 15-19 under 35 U.S.C. 102(e) as being anticipated by Porras et al US Patent 6,321,338.

Although the Examiner in the summary of the rejection indicated that only claims 1-6, 9-13, 15 and 16 were rejected over Porras in the body of the rejection the examiner also rejected claims 17-19 over Porras. Thus Applicant treats this rejection as a rejection of claims 1-6, 9-13, and 15-19.

The claims are distinguished over Porras. Claim 1 for instance is distinct over Porras. Claim 1 recites ... a control center ... that is coupled to a network... including a communication device to receive data from a plurality of monitors, dispersed through the network, with the monitors sending data collected from the network over a hardened, redundant network. At least these features are not described by Porras.

The examiner takes the position that Porras at Col. 8 lines 13-21 teaches "a plurality of monitors over a hardened, redundant network." Porras has no such teachings at the cited passage or elsewhere. Rather, Col. 8 lines 13-21 describe:

> The analysis engines 22, 24 receive large volumes of events and produce smaller volumes of intrusion or suspicion reports that are then fed to the resolver 20. The resolver 20 is an expert system that receives the intrusion and suspicion reports produced by the analysis engines 22, 24 and reports produced externally by other analysis engines to which it subscribes.

There is nothing in the cite passage relied on by the examiner or elsewhere in Porras that suggests much less describes a plurality of monitors over a hardened, redundant network or "a control center including a communication device to receive data from a plurality of monitors,

dispersed through the network, with the monitors sending data collected from the network over a hardened, redundant network."

Moreover, the architecture of the system claimed in claim 1 is distinct from that taught by Porras. In Porras each monitor 16 includes a resolver 20 (Col. 4 lines 55-56). The Examiner identified the resolver 20 as the central controller (Office Action page 2 paragraph 3). Accordingly, in Porras the resolver is a functional unit of the monitor, whereas in claim 1 the central controller is a part of a larger system that includes a plurality of monitors that are coupled to the central controller. Therefore, Porras neither discloses nor suggests a system that includes a central controller to coordinate thwarting attacks on a victim data center with the central controller system including a communication device to receive data from a plurality of monitors dispersed through the network, and a process that executes to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic.

Accordingly claim 1 and claims 9 and 18, which generally correspond to claim 1 are distinct over Porras. Claim 18 further distinguishes since it clearly is drawn to instructions to receive data from a plurality of monitors, dispersed through a first network that is coupled to the victim data center, with the monitors sending data collected by the monitors from the first network to a control center over a hardened, redundant, second different network.

Dependent claims 2-6, 10-13, 15, 16, 17 and 19 serve to further distinguish over Porras.

For instance claim 2 recites that the control center comprises an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center and claim 3 recites that the data analyzed by the control center is sampled packet traffic and/or accumulated and collected statistical information about network flows.

Although Porras discusses aspects of data collection and statistical analysis, to the extent that Porras discloses such functions as claimed (which Applicant does not concede), Porras does not perform those functions with the control center. Therefore, claims 2 and 3 serve to further distinguish over Porras. Claim 4 likewise distinguishes by reciting that the control center aggregates traffic information and coordinates measures to locate and block the sources of an attack.

Claim 5 calls for the control center being a hardened site. The examiner considers Porras as teaching this at col. 2 lines 8-10 in the discussion concerning the network entity being a virtual private network. Applicants contend that the network entity referred at Col 2 lines 8-10 is the network entity set out at Col 1 lines 45-46, which corresponds to a network forwarding device, e.g., router or switch being monitored, rather than one of the monitors disposed in the network to examine packets handled by the entity. This is confirmed by examination of FIG. 1 and Col. 3 lines 41-44 where Porras discloses network entities as distinct from monitors and as including gateways, routers, etc. Hence, Porras does not disclose a control center and does not disclose a control center being a hardened site.

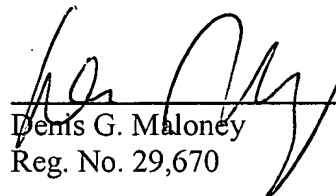The Examiner rejected claims 7-8 and 14 under 35 U.S.C. 103 as being obvious over Porras in view of Hill

Hill does not solve any of the deficiencies in Porras as noted above. Therefore, for at least the reasons discussed above these claims are also allowable over this combination of references.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 5/20/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

20851880.doc